AOIT Computer Systems

Lesson 5

Basic Data Protection

Student Resources

|  |  |
| --- | --- |
| Resource | Description |
| Student Resource 5.1 | K-W-L Chart: Essay Disaster Scenario |
| Student Resource 5.2 | Reading: Windows User Accounts |
| Student Resource 5.3 | Tutorial: Creating a User Account |
| Student Resource 5.4 | Reading: Protecting Your Data |
| Student Resource 5.5 | Scavenger Hunt Worksheet: Protecting Data |
| Student Resource 5.6 | Writing Assignment: Data Protection User Guide |

Student Resource 5.1

K-W-L Chart: Essay Disaster Scenario

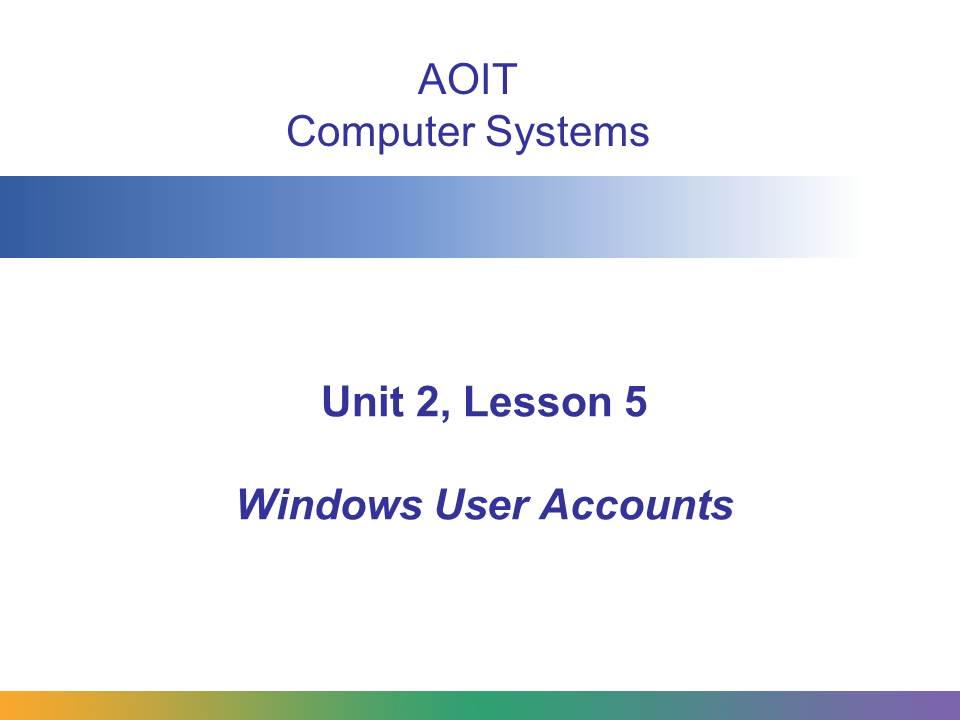
Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: If your friend had acted yesterday, how could she have saved her essay from getting wiped out? Use this chart to fill in your ideas and details about things you already know about how to protect data on a computer. Put what you already know in the “K” column. An example is provided.

|  |  |  |
| --- | --- | --- |
| What I Know | What I Want to Know | What I Learned |
| My friend should have backed up her essay. | How exactly do you do that? | Copy important files like this to a flash drive, CD-ROM, or online backup server every day. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Student Resource 5.2

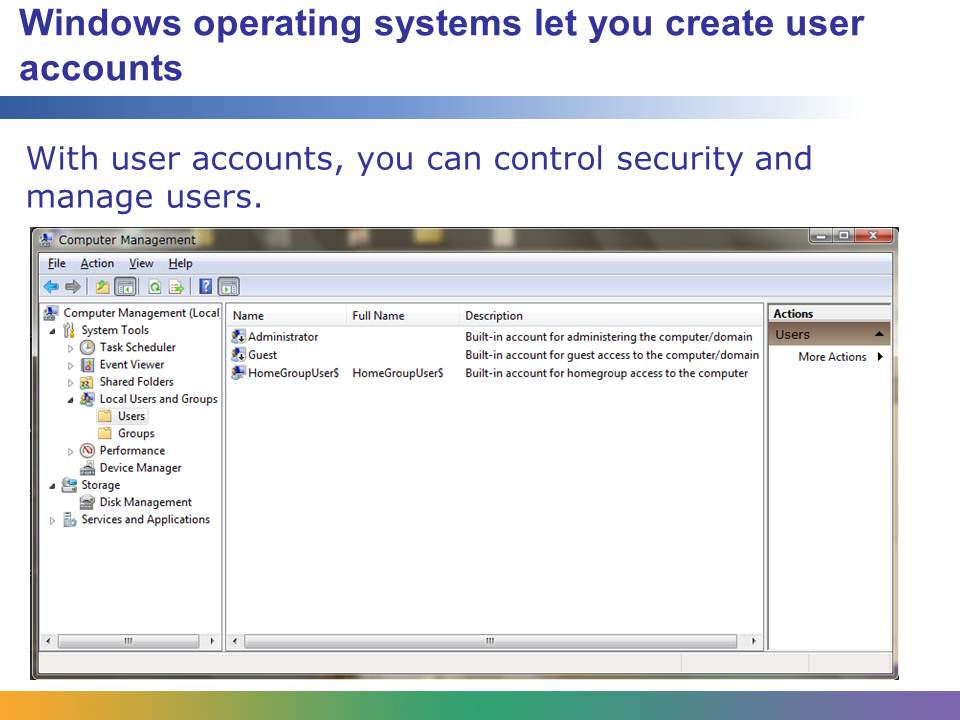
Reading: Windows User Accounts



This presentation explains ways you can use Windows 7 and Windows XP user account privileges to protect data on your home computer. Windows user accounts allow many people to share one computer. They allow some users to control the full environment and offer other users safer, more easy-to-use features.

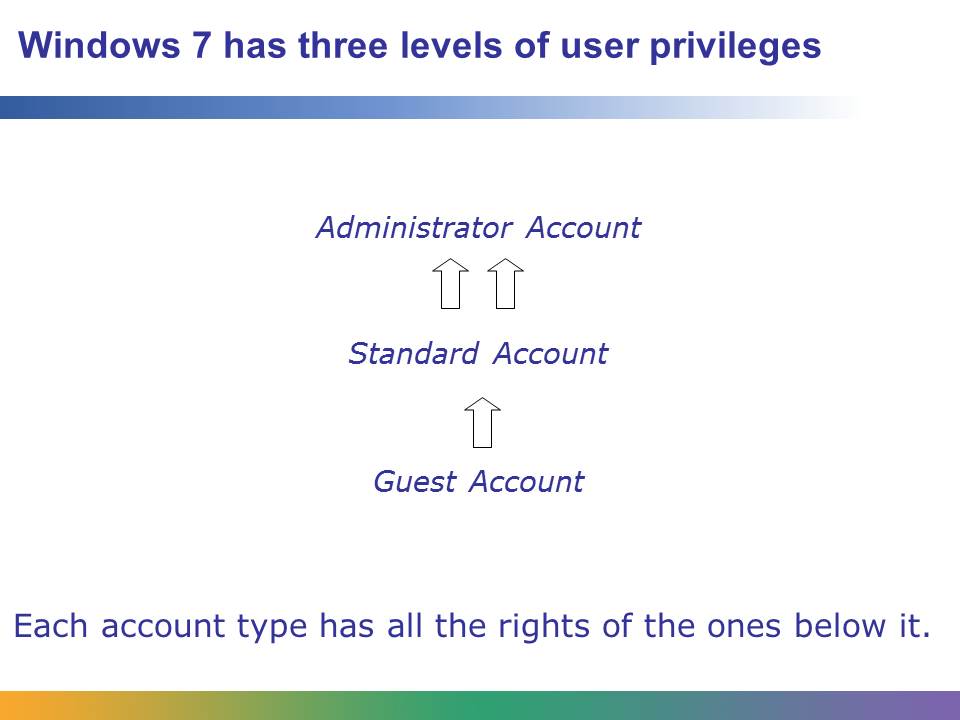
The main topics include the following:

* Different types of user accounts and what privileges they provide
* Ways to protect data on a peer-to-peer network by creating user groups



In Windows operating systems, you can create user accounts to manage the rights that people have when using a computer. Creating user accounts also keeps the computer more secure by controlling access. User accounts determine which files and programs users can access and what types of changes users can make to the computer.

With user accounts, several people can easily share a single computer. Each person can have a separate user account with unique settings and preferences, such as a desktop background or screen saver.



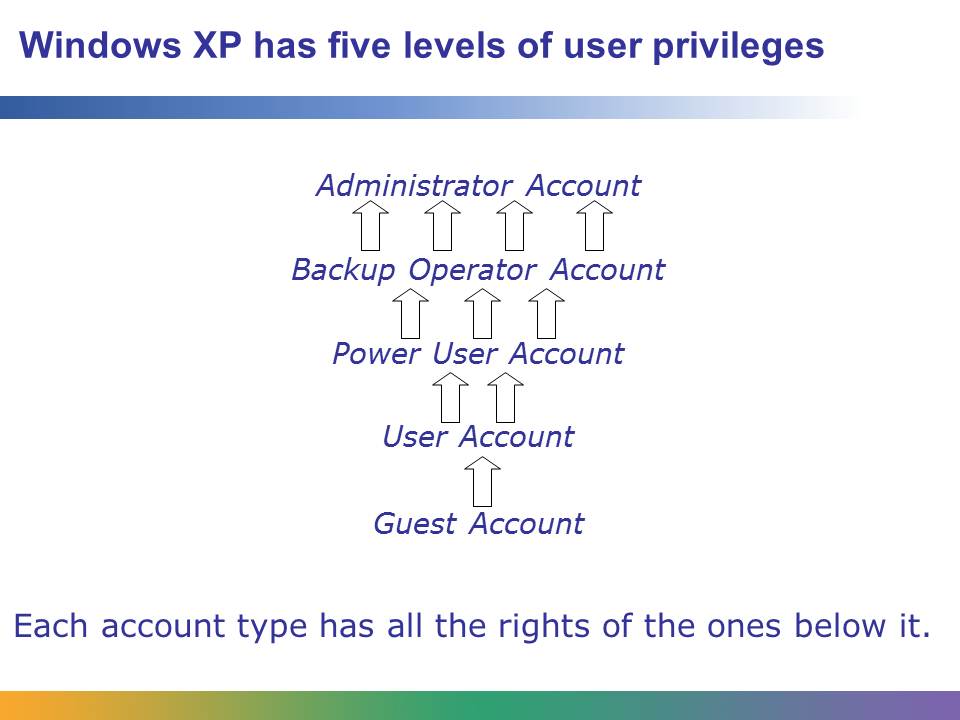
Windows 7 uses three basic account types that all have specific access, privileges, and features. These account types are: administrator, standard user, and guest. Their permissions are similar to the permissions they had in Windows XP.

The administrator account has the most permissions of all the account types. An administrator can change or modify all files within Windows, adjust system defaults and Windows settings, and even manage other users. If you only have one account on your PC, it is most likely the administrator account.

A standard user account is a basic account type that is more restricted than an administrator account. Standard users cannot adjust certain files, cannot change deep system values, and cannot manage other users.

The guest account is the most restricted of all account types and is normally used for public computers that have several users on a frequent basis. They have no password and can only access and save files. They can make no changes to their account types or to the system.

To see if you are logged in with the administrator account, open the Control Panel and click Add or Remove User Accounts. There should be an account login picture and account name. If you are logged in as an administrator, the word *Administrator* will appear directly below the account name.



If several people use one computer, you can control what files and actions those users have access to. This is helpful if you need to assign certain tasks to different people, such as creating backups.

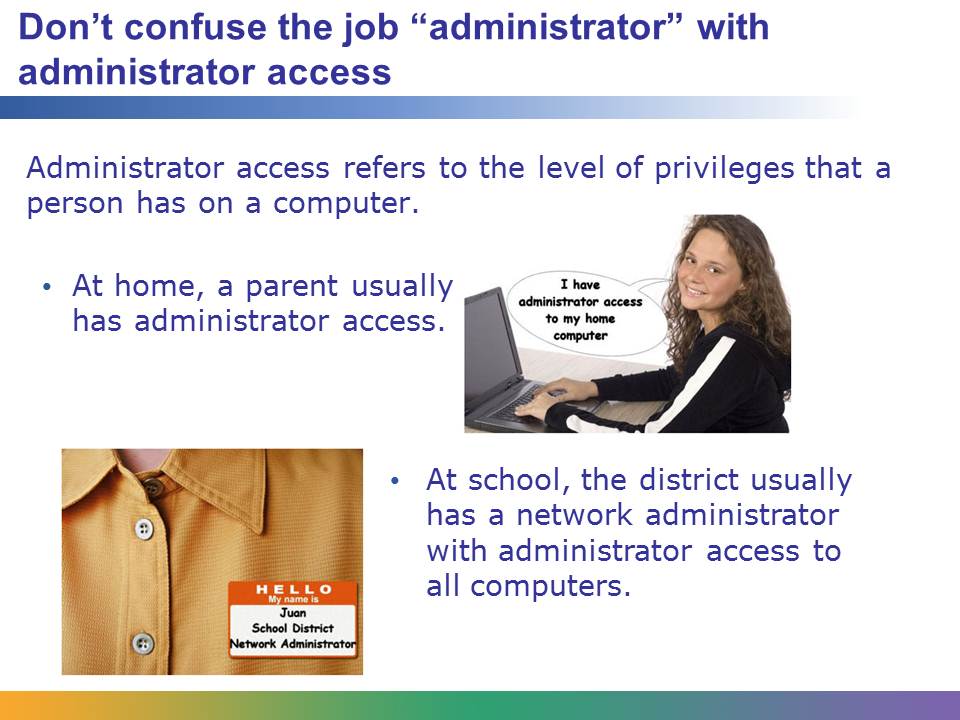
In Windows XP, the person with all possible privileges is called the *local administrator* for the computer. This person has administrative user account privileges, which allows him or her to maintain the operating system, control user access to the computer (add/delete users, reset other people’s passwords, and so on), and back up and restore the system. The local administrator is also responsible for installing new software on the computer.

The user account type of next responsibility is that of *backup operator*. This person can back up and restore computer files, but can’t change security settings.

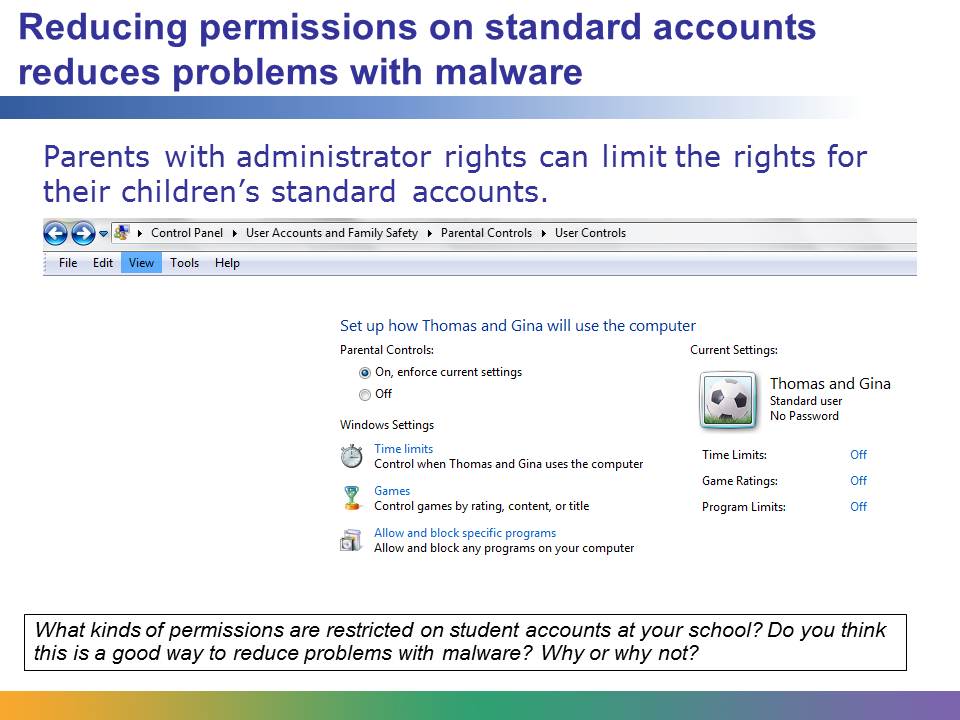
People with *power user* privileges can create user accounts for other people on a peer-to-peer network but can only modify the accounts they create.

People with *user* accounts can perform common tasks such as running applications and printing to local and network printers. They can also change their own password.

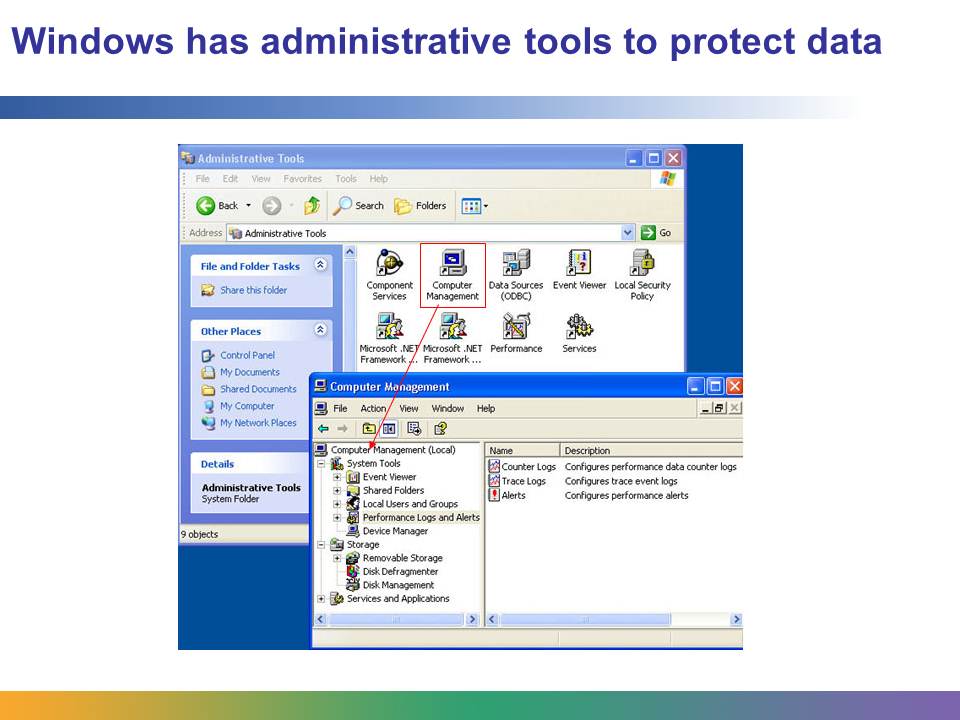
There is also a built-in *guest user* account type that allows occasional or one-time users to log in to a computer, but these users are granted very limited abilities. They have no password and can only access and save files. They can make no changes to their account types or to the system.



When having a discussion about Windows user account privileges and user account types, it is easy to confuse the person (the administrator) with the account type (administrator access). Just make sure as you forge ahead that you keep the two straight in your mind. One is a person’s job, and the other describes a level of user privileges. Every computer has at least one person with administrator access, and this person has full privileges on the computer. It’s important for the administrator to remember the administrator password. If the computer ever needs to be repaired, the person repairing it will need the administrator password.

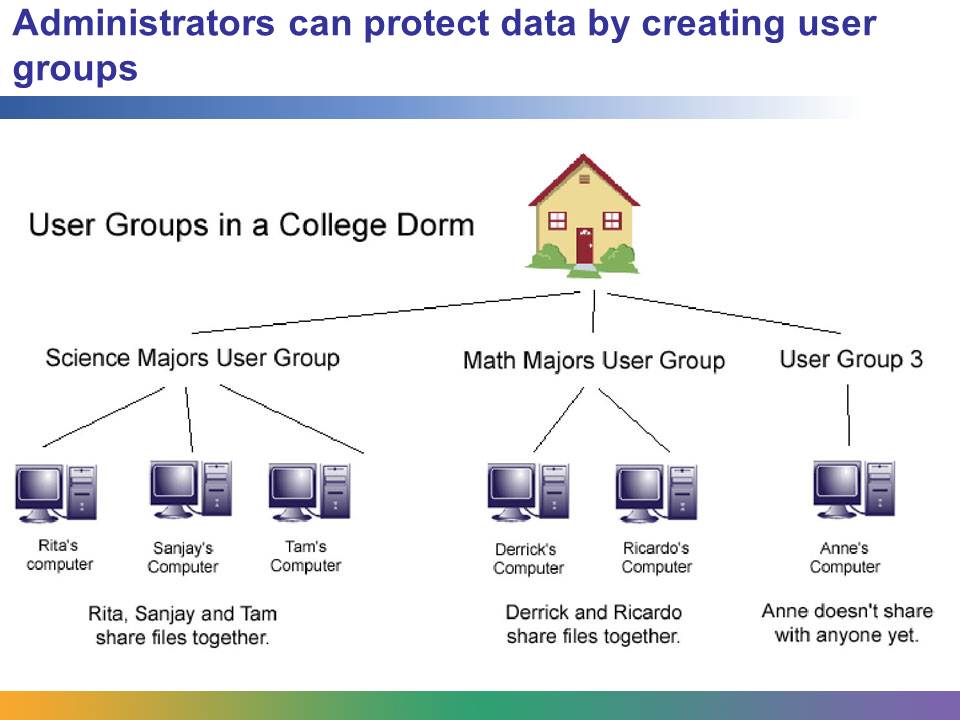


Reducing a user’s level of permissions is a great way to reduce chances of having problems with malware. For example, on a home computer, the parents may have full administrator rights, and the children may have much more restricted accounts so that they can’t install anything without permission from the parents (the administrators, in this case).



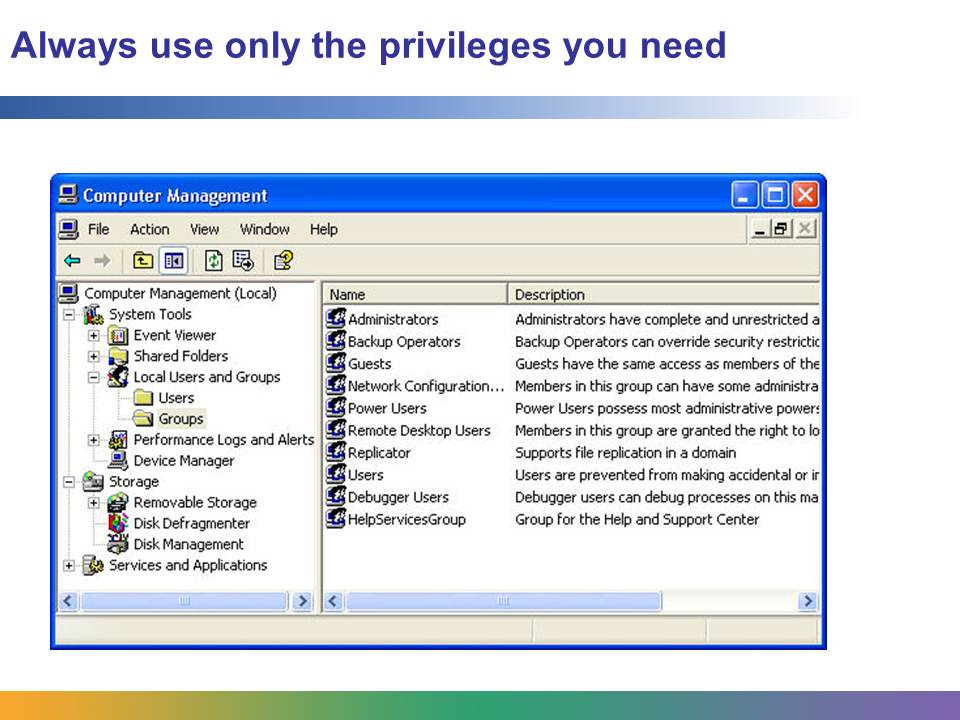
A person with administrator rights can protect data by using Control Panel tools to perform actions such as the following:

* Collect real-time data about memory, disk usage, processors, and networks in a graph or a report.
* Automate administrative tasks such as updating security software or running a full system scan.
* If anything goes wrong and the system becomes unstable, perform system recovery functions that bring the system back to its last stable state. This is very important part of data protection.



If computers are hooked together to form a peer-to-peer network, people with administrator user accounts can create user groups that will help some people share files—and keep others out.

For example, the data that belongs to the Science Majors User Group cannot be accessed by the people in the Math Majors User Group.



There’s a principle known as the Principle of Least Privilege. This refers to the fact that it’s important for all users to be logged on to the computer with *only* the privileges they need to do their jobs.

This is because hackers love people to be working on their computer with administrative privileges—that’s the type of access they need to amend security settings and control another person’s system.

By logging in to your system with the least amount of privileges you need on a computer, you’re protecting both your system and your data. You can see on this slide the different user account types that are available.

Student Resource 5.3

Tutorial: Creating a User Account

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: Imagine you have a friend who often comes to your house and asks to use your computer. It’s okay for your friend to use the computer, but you need to create a guest account for her so that she will have access only to what she needs.

Working on a computer where you have administrator rights, use the help available from the Help and Support menu on your computer to create a new user account, and associate this account with the Guests group.

Note: If you are using Windows 7, the procedure for guests is a bit different. From the Start icon, type Guest user in the Search box, and you will learn how to have a Guest user with Windows 7.

1. From the Start menu, click Help and Support.
2. Type *Create a new user account* in the Search box of the window that displays.
3. In the list of tasks that displays, click “Create a new user account” (or “Add a new user to the computer”).
4. Follow the instructions to create the user account.
5. When the account is created, the account name will display in the list of users (under Computer Management > System Tools > Local Users and Groups > Users). Check to make sure your new user displays in this list. (Note: These instructions will not apply to users using Windows XP Home Edition. For Home Edition users, you will need to use the User Accounts Tool in the control panel.)
6. By default, the new user is a member of the Users group. You need to add this user to the Guests group and delete this user from the Users group:
   1. Double-click the user name; the Propertiesbox will display.
   2. Click the “Member of” tab.
   3. Select Users in the list, and click Remove.
   4. Click Add to add the Guests group.
   5. In the “Enter the object names to select” box, type *Guests*, and then click OK.
   6. Click OK in the Properties box to complete the procedure.
7. To check that your friend is now a member of the Guest group, double-click the user account to display the Properties box, and then click the “Member of” tab. It should say “Guests.”

Student Resource 5.4

Reading: Protecting Your Data

Having a local administrator user account on your computer means you have the rights and privileges to change many settings on the computer that other types of users on the same computer do not. The first person who sets up your computer is automatically assigned the role of local administrator, but you can change that or add others. You just need to keep one local administrator account on your computer so that the very important administrative functions are always covered. On a home PC, often there is only one account created, with no password. By default, this account has administrator privileges.

There are many ways to protect data on a PC with a local administrator user account. But a lot of people don’t remember to protect data until five minutes after an electrical surge, a moment of carelessness, or the wipeout of their data by a hacker. And then it’s too late. You should remember to perform a number of tasks on a regular basis to keep your data safe. Here are seven of them.

Keeping Your Operating System Up-to-Date

Hackers say that any operating system is vulnerable in some way. Tens of dozens of new cyberattacks are launched every day on personal computers, mom-and-pop websites, banks, and even the Pentagon. The makers of your Windows OS know this and are constantly closing holes in their code when they discover new attacks. Even though Microsoft officially releases updates on Tuesday of every week, it’s important that you set up your system to automatically accept updates from Microsoft every day. There might be emergency fixes during the week.

Backing Up Your Data and Your OS

When you first get your computer, it’s very important to create system recovery disks so that they can be used to restore your computer if your system becomes unstable or won’t start. It is very important to keep these disks (and the Windows CD that sometimes comes with your computer) safe and scratch free.

It is also important to back up your data. The whole data-backup process can take you less than 10 minutes a week when you use the Microsoft XP Backup Wizard. The Backup Wizard saves all users’ personal settings, preferences, email, and data to some external drive, such as a CD-R, CD-RW, flash drive, or second hard drive (these days the easiest solution for a single computer is generally a large external hard drive).

You can also use third-party software (software that’s made by other companies) to back up the Windows system information.

Another option is to copy your important files to a CD-ROM, DVD-ROM, external hard drive, or flash drive every day. If your system crashes, you’ll still lose your personal settings, preferences, and email, but you won’t lose your essay, for example. You can also enable a scheduled task (in System Tools) to run a nightly automatic update.

Online backup offers an added level of protection. Online backup services offer the advantage of securely storing your files at an off-site server location. This means your data stays intact and available even if your local computer or backup is stolen or the premises are struck by fire, flood, or some other type of disaster. As “cloud computing” becomes more prevalent, there are many products on the market that provide cloud backup services. Dropbox, idrive, and Microsoft’s Sky Drive, are some examples. All of these online backup services regularly upload new and changed files to a secure server. Each online backup product has a different set of features, so it is important to examine the product carefully to choose one that meets your needs.

Creating Strong Passwords

The basic characteristics of strong passwords are that they should be random (no rules or methods to the characters you choose), and they shouldn’t be easily associated with real words. Avoid dictionary words, letter or number sequences, user names, or information such as names or dates. Make your passwords at least eight characters in length.

Strong passwords include a mixture of the following elements:

* Numbers
* Non-alphanumeric characters (` ~ ! @ # $ % ^ & \* - + = | \ { } [ ] : ; " ' < > , . ? / )
* Uppercase letters
* Lowercase letters

If you know a lot about local administrator privileges, you can use special administrative tools to set the password policy for the computer. For example, you can force users to create a password that is at least a certain number of characters (for example, eight), require that a password contain both numbers and letters, or force users to change their password every so often.

Password strength is important but does not guarantee security. Strong passwords can still be beaten by insider attacks, phishing, keystroke logging, social engineering (tricking someone into giving up their password), and even dumpster diving (finding a scrap of paper you threw away with your password on it).

The practice of password guessing by running a simple program that tries all possible combinations can be referred to as *brute-force* password generation. Simple brute-force programs running on a 3 GHz processor can guess approximately 3 million passwords a second. An even easier program for hackers to run is one that tries every word in a dictionary. However, a 10-letter password that uses numbers, punctuation, and uppercase and lowercase letters would take approximately 632,860 years to guess, assuming purely random passwords. Randomness is a huge element to creating strong passwords.

Deleting Your Trash/Recovering Deleted Files

Removing a file from your computer by deleting (right-click the file name and select Delete) simply moves the file to your Recycle Bin. Anyone with access to your account on the computer can open your Recycle Bin, find the file you thought you deleted, and open it.

By deleting your trash (right-click on the desktop Recycle Bin and select Empty Recycle Bin) on a regular basis, perhaps every week, you make it much more likely your discarded file will truly disappear.

However, even if you delete your trash, it is possible to use data recovery tools to bring back files that have been deleted. The sooner you try to get the file back, the better, because Windows won’t overwrite the data right away. But the more you save other files onto your hard drive, the more likely it is that your original data will be overwritten, which makes it difficult to recover.

Certain freeware is available to help bring back deleted files. You can also purchase third-party software products that will help.

Encrypting Files

Encrypting a file is like turning its content into complicated spy code so that only the computer with the decoder key can read the message. The computer sending the data changes it according to a mathematical formula (an algorithm), and the decoding computer uses a complementary “key” to decode the message and turn it into readable information. By encrypting a file, you’re protecting it from being read by someone who doesn’t have the key.

Microsoft Windows XP includes the Encrypting File System (EFS), which has the ability to encrypt data by setting up special encrypted format and folders that you can drag and drop files into. There is also third-party media encryption (or disk encryption) software that encrypts your whole hard disk. To do this, the software saves your data in encrypted form so that anyone who steals your files and tries to open them on a different computer cannot make sense of the information, since they don’t have the encryption key. This is especially important on portable computers because they are so easily lost or stolen.

You can even buy external hard drives that automatically encrypt everything that’s saved to them.

Different kinds of businesses require different strengths of encryption services. For example, data from a bank is going to require a stronger (more expensive/complicated) system than you’d probably need for protecting files on your home computer.

Hiding Files

If your computer is set up to share files on the Internet, or if you share a computer with someone, you may have files or folders you want to hide. One way to do this is to purchase a program to password-protect them.

Another less expensive way is to log in with a local administrator user account and hide your folders so that they can’t be seen. This involves using the Windows XP folder option “Do not show hidden files and folders.” This method is simple but probably wouldn’t stop anybody who knows a lot about computers. However, it would probably stop your ordinary friend or family member.

System Recovery

When you first get your computer, besides making recovery disks, you should enable your system restore so that the *registry* (the directory that stores the settings and options for your operating system) can be rolled back to its last stable state in the event of a problem. Then, if your system is unstable or your operating system doesn’t start, you can attempt to recover both the system and the data on the computer.

There are two ways to restore a system in Windows XP. The first is a standard recovery. A standard recovery is also known as a *partial recovery*, because it recovers the OS, your drivers, and the programs that originally came on your computer without losing any data files on the system.

A full recovery completely erases and reformats the hard drive, and it reinstates the OS, programs, and drives from the recovery disks—which you were smart enough to make when you first got your computer.

Student Resource 5.5

Scavenger Hunt Worksheet: Protecting Data

Student Names:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: Your teacher will assign one of the following data protection methods to your group. Consult your reading and at least two Internet sources to answer the questions about your data protection method. You can write your answers and list your resources on this worksheet.

**I. Keeping Your OS Up-to-Date**

1. Why do you need to keep your OS up-to-date?
2. How often should you do it?
3. What steps do you need to take to find out whether your OS is up-to-date?
4. If it’s not up-to-date, what steps do you take to update your OS?

Resources we used:

**II. OS Backups**

1. When should you back up your operating system?
2. What steps does one take to create a system recovery disk?
3. Explain the steps you need to take to bring an OS back to its pre-crash state.

Resources we used:

**III. System Restore**

1. What steps does a person with administrator privileges need to take to restore a system that is unstable?
2. To get a computer back to its pre-crash state, what would you have to do besides a standard recovery?
3. Describe what you can do with the one you selected, how much it costs, and where you can buy it.

Resources we used:

**IV. Data Backups**

1. Why do you need to back up your data?
2. How often should you do it?
3. List two things you could do on your computer to save your data from loss.
4. Write down the steps that a person would need to follow to accomplish these tasks.
5. What steps does one take to create a system recovery disk?

Resources we used:

**V. Creating Strong Passwords**

1. Why are strong passwords important?
2. What are the rules for creating strong passwords?
3. Name three things strong passwords protect against.
4. Give two examples of strong passwords, and explain why they’re good ones.

Resources we used:

**VI. Encrypting Files**

1. Why might you want to encrypt files?
2. Find two ways to encrypt files.
3. How does one of them work?
4. Describe what you can do with something you selected to encrypt files, how much it costs, and where you can buy it.

Resources we used:

**VII. Hiding Files**

1. Why might you want to hide files on a computer?
2. Find two solutions you can use to hide files on a computer.
3. How does one of them work?
4. Describe what you can do with the one you selected, how much it costs, and where you can buy it.

Resources we used:

Student Resource 5.6

Writing Assignment: Data Protection User Guide

Student Names:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: Imagine you are explaining data protection procedures to someone who knows nothing about how to protect data. Your assignment is to write a page for a data protection user guide explaining the data protection method that you researched. Your page will be collated with pages from your classmates, who researched other data protection topics, to create a complete user guide. You will review each other’s subject areas to make sure what you’ve written makes sense.

Your page should include the following types of information:

* Why this data protection method is important
* A step-by-step procedure for protecting data using this method
* Instructions on how often and when to perform this data protection procedure
* The resources you used to find this information

The example on the next page shows how to structure your page and the kinds of information you should include.

User Guide Example

This example is a page from a user guide that provides instructions to someone who has purchased a cell phone. The guide has several pages, one for each of the various tasks that a new cell phone user must perform. For example, there is a page on adding contacts, a page on setting up voice mail, and a page on ring tones, and so on. This example shows what the page for adding contacts looks like. The page you write for the data protection user guide should have the same elements (a title, information about why and when users want to perform the task, a list of steps to perform the task, instructions on how often and when to perform this data protection procedure, and a list of resources where you got your information).

**Adding Contacts to Your Cell Phone**

Adding contacts to your cell phone makes it easier to contact the people you call most often. If you don’t remember a person’s phone number and don’t have it handy, you can still call that person. It makes calling both quick and easy.

The easiest way to add a new contact is to save the sender’s information when someone calls you or sends you a text message. You can also enter a new contact from scratch when you meet someone and don’t want to forget their number.

**Note**: The following steps are taken from the iPhone User Guide. The steps you would need to perform on your own phone might be different, depending on the type and model of phone you use.

**To add a recent caller’s information:**

* + Tap the Recents icon.
  + Then tap the arrow  next to the number.
  + Tap “Create New Contact” and enter the caller’s information, or tap “Add to Existing Contact” and choose a contact.

**To add a new contact:**

1. Choose Contacts. 
2. Tap **+**, then enter the contact information.

**To add an email recipient to your contacts:**

1. Tap the message and, if necessary, tap Details to see the recipients.
2. Then tap a name or email address and tap “Create New Contact” or “Add to Existing Contact.”

**Resources for this guide:**

* “Adding Contacts to Cell Phone” reading
* http://manuals.info.apple.com/en/iphone\_user\_guide.pdf
* [http://www.mobileusa.com](http://www.mobileusa.com/)
* [http://www.samsung.com](http://www.samsung.com/)